AMENDMENTS

In The Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claim 1 (currently amended) A cryptographic communication system comprising:

a plurality of user communication interfaces, each of said communication interfaces ~~interface~~ including:

a data receiver;

a string generator;

a data processor connected to said string generator; and

a memory connected to said string generator, said memory having stored a unique seed value and a common seed value,

wherein the data processor processes data received by the data receiver using data string generated by the string generator,

wherein the unique seed value for each of said plurality of user communication interfaces are unique to the respective communication interface, and wherein the common seed value stored in the memory of each of said plurality of communication interfaces is common to all of the plurality of communication interfaces, and

wherein the string generator generates data string using the unique seed value if the data received by the data receiver is unicast data intended to be received by one of said plurality of communication interfaces, and generates data string using the common seed value if the data

received is designated as multicast data intended to be received by all of said plurality of communication interfaces ; and

a master station, said master station including:

a data transmitter;

a second string generator;

a second data processor connected to said second string generator; and

a second memory connected to said second string generator, said second memory having stored ~~said~~ each of the unique seed value stored in the plurality of communication interfaces and the common seed value,

wherein the second data processor processes data to be transmitted by the data transmitter using data string generated by the second string generator, and

wherein the second string generator generates data string using one or more of the unique seed values if the data to be transmitted by the data transmitter is intended to be received by select ones of said plurality of communication interfaces, and generates data string using the common seed value if the data to be transmitted is intended to be received by all of the plurality of communication interfaces.

Claim 2 (original) The cryptographic communication system according to claim 1,

wherein said string generator is a pseudo-random string generator, and

wherein said second string generator is a pseudo-random string generator.

Claim 3 (previously presented) The cryptographic communication system according to claim 1,

wherein each of said plurality of user communication interface further includes a key block formation device, and

wherein said master station further includes a second key block formation device.

Claim 4 (previously presented) The cryptographic communication according to claim 1, wherein each of said plurality of user communication interface is connected to said master station through a communication network.

Claim 5 (previously presented) The cryptographic communication according to claim 1, wherein each of said plurality of user communication interface communicates with the master station via a wireless network.

Claims 6-7 (canceled)

Claim 8 (previously presented) The cryptographic communication system according to claim 1,

wherein said second memory of said master station stores a user address value for each of said plurality of user communication interface.

Claim 9 (currently amended) The cryptographic communication system according to claim 8, wherein each of the unique seed values stored in said second memory is referenced to by the user address value corresponding to the user communication interface in which the unique seed value is stored.

Claim 10 (previously presented) The cryptographic communication system according to claim 1,

wherein said second memory of said master station stores a user identification for each of said plurality of user communication interface.

Claim 11 (currently amended) The cryptographic communication system according to claim 10, wherein each of the unique seed values stored in said second memory is referenced to by the user identification corresponding to the user communication interface in which the seed value is stored.

Claim 12 (currently amended) The cryptographic communication system according to claim 1,

wherein ~~each of said plurality of user communication interface further includes~~ said data processor is a data decryptor, and

wherein said ~~master station further includes a master~~ second data processor is a data encryptor.

Claim 13 (currently amended) The cryptographic communication system according to claim 1,

wherein each of said plurality of user communication interface further includes a data encryptor, and

wherein said master station further includes a ~~master~~ data decryptor.

Claims 14-15 (canceled)

Claim 16 (currently amended) A method of cryptographic communication comprising the steps of:

storing in a memory a unique seed and a common seed;

receiving a signal;

detecting whether the signal is a unicast signal or a multicast signal;

generating ~~data strings~~ a data string using the unique seed if the signal is detected to be a unicast signal, and generating a data string using the common seed if the signal is detected to be a multicast signal;

forming a decryption key using ~~at least one of said data strings~~ the generated data string; and

~~receiving a signal; and~~

decrypting the received signal using said decryption key.

Claim 17 (currently amended) The method of cryptographic communication according to claim 16, wherein, when a series of data strings are generated ~~said data strings are~~ generated from either the unique seed or from the common seed, the series of data strings are generated in a pseudo-random order.

Claim 18 (original) The method of cryptographic communication according to claim 16, further comprising the step of determining whether the received signal is encrypted.

Claims 19-23 (canceled)

Claim 24 (original) The method of cryptographic communication according to claim 16, further comprising the step of transmitting a user address or a user identification.

Claim 25 (currently amended) A method of cryptographic communication comprising the steps of:

storing a unique seed and a common seed;

receiving a signal to be transmitted;

generating ~~data strings~~ a data string using one of said unique seed and said common seed, wherein the data string is generated from the unique seed if the signal to be encrypted is to be transmitted to a single recipient, and generated from the common seed if the signal to be encrypted is to be transmitted to more than one recipient;

forming an encryption key using the generated data string ~~at least one of said data strings~~;

encrypting ~~a~~ the signal using said encryption key ~~keys~~; and

transmitting the signal.

Claim 26 (currently amended) The method of cryptographic communication according to claim 25, wherein, when a series of data strings are generated ~~said data strings are~~ generated from either the unique seed or from the common seed, the series of data strings are generated in a pseudo-random order.

Claim 27 (currently amended) The method of cryptographic communication according to claim 25, further comprising the step of determining whether to encrypt the signal prior to transmitting the signal ~~signal~~.

Claim 28 (canceled)

Claim 29 (currently amended) The method of cryptographic communication according to claim 25, further comprising the step of storing one of a user address and a user identification corresponding to the unique seed.

Claims 30-37 (canceled)

Claim 38 (currently amended) A computer readable medium including executable instructions for causing a processor to perform a method of cryptographic communication, said method comprising the following steps:

storing in a memory a unique seed and a common seed;

receiving a signal;

detecting whether the signal is a unicast signal or a multicast signal;

generating ~~data strings~~ a data string using the unique seed if the signal is detected to be a unicast signal, and generating a data string using the common seed if the signal is detected to be a multicast signal;

forming a decryption key using ~~at least one of said data strings~~ the generated data string; and

~~receiving a signal; and~~

decrypting the received signal using said decryption key.

Claim 39 (currently amended) The computer readable medium of claim 38, wherein, when a series of data strings are generated ~~said data strings are~~ generated from either the unique seed or from the common seed, the series of data strings are generated in a pseudo-random order.

Claim 40 (original) The computer readable medium of claim 38, wherein said method further comprises the step of determining whether the received signal is encrypted.

Claims 41-46 (canceled)

Claim 47 (original) The computer readable medium of claim 38, wherein said method further comprises the step of transmitting a user identification.

Claim 48 (currently amended) A computer readable medium including executable instructions for causing a processor to perform a method of cryptographic communication, said method comprising the following steps:

storing a unique seed and a common seed;

receiving a signal to be transmitted;

generating ~~data strings~~ a data string using one of said unique seed and said common seed, wherein the data string is generated from the unique seed if the signal to be encrypted is to be transmitted to a single recipient, and generated from the common seed if the signal to be encrypted is to be transmitted to more than one recipient;

forming an encryption key using the generated data string ~~at least one of said data strings~~;

encrypting ~~a~~ the signal using said encryption key ~~keys~~; and

transmitting the signal.

Claim 49 (currently amended) The computer readable medium of claim 48, wherein, when a series of data strings are generated ~~said data strings are~~ generated from either the unique seed or from the common seed, the series of data strings are generated in a pseudo-random order.

Claim 50 (previously presented) The computer readable medium of claim 48, wherein said method further comprises the step of determining whether to encrypt the programming signal prior to transmitting said signal.

Claims 51-52 (canceled)

Claim 53 (currently amended) The computer readable medium of claim 52, wherein said method further comprises the step of storing one of a user identification and a user address that correspond with the stored unique seed.

Claims 54-60 (canceled)